5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/847,757	05/02/2001	James B. Pritchard	PRIT01-00003	6039

7590 10/01/2004

Biggers & Ohanian, PLLC
5 Scarlet Ridge
Austin, TX 78737

EXAMINER	
JACKSON, JENISE E	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/847,757	**Applicant(s)** PRITCHARD ET AL.	
	Examiner Jenise E Jackson	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24,27,29 and 31-45* is/are rejected.

7)☒ Claim(s) *25,26,28,30,46 and 47* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *052001*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 1-20, 37-47 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim 9, which is dependent from 8, which is dependent from independent claim 1; also, independent claim 20, is also rejected under 112. Claim 42 which is dependent which depends on independent claim 37. Claims 9, 20, and 42 include the limitation of hardware control switch, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. There is no mention in the specification of a "hardware control switch". In the specification on page 12, disclosed is a data transfer switch, and a peripheral switch. In the specification on page 21, disclosed is a HPC(101) that operates the peripheral switch through peripheral switch port on HPC. There is no mention of a hardware control switch capable of causing the peripheral switch of the second computer system to switch control of the computer peripheral. Therefore, the claims 1-20, and 37-47 are rejected.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-4, 12-15, 31-33, 36-39 are rejected under 35 U.S.C. 102(b) as being anticipated by Schnurer et al(5,842,002).

5. As per claims 1, 31, Schnurer et al. discloses protecting a first computer system(i.e. file server) from an intrusion such as a computer virus or an unauthorized access(see col. 6, lines 41-49), a second computer system(i.e. trapping device) coupled to said first computer system(i.e. file server)(see col. 6, lines 41-49), said second computer system capable of detecting said intrusion before said intrusion reaches said first computer system(see col. 6, lines 63-67, col. 7, lines 1-18).

6. As per claims 2, 32, Schnurer et al. discloses wherein said second computer system is capable of deleting said intrusion after said second computer system detects said intrusion (see col. 8, lines 27-35).

7. As per claim 3, Schnurer et al. discloses that the trapping device monitors for data streams where the streams pass to the emulation chamber were intrusion/viruses are allowed to execute without infecting the first computer(i.e. file server), if a virus is detected in Schnurer et al. the file can be deleted, thus Schnurer discloses, wherein said second computer system is

capable of deleting said intrusion by erasing data within said second computer system(see col. 6, lines 63-67, col. 7, lines 1-18, col. 8, lines 27-35).

8. As per claims 4, 33, Schnurer et al. discloses wherein said data erased by said second computer system(see col. 8, lines 27-35) includes one computer software program within said second computer system(see col. 6, lines 8-22).

9. As per claims 12, 36, Schnurer et al. discloses wherein the second computer system(i.e. virus trap) is capable of receiving all external computer communications that are directed to the first computer system(i.e. file server)(see col. 6, lines 41-49).

10. As per claims 13, 37, Schnurer et al. discloses a virus trap computer system(see col. 6, lines 41, 50, 63) for protecting a host computer system from an intrusion such as a computer virus(see col. 6, lines 41-49), the virus trap computer system including, an embedded personal computer coupled to the host computer system(see col. 6, lines 8-49), the embedded personal computer capable of receiving all external computer communications that are directed to the host computer system(see col. 6, lines 41-49), and capable of detecting the intrusion before the intrusion reaches the host computer system(see col. 6, lines 41-49, 64-67, col. 7, lines 1-18).

11. As per claims 14, 38, Schnurer et al. discloses wherein the virus trap computer system is capable of deleting the intrusion by erasing data within the virus trap computer system(see col. 7, lines 1-8, col. 8, lines 27-35).

12. As per claims 15, 39, Schnurer et al. discloses wherein the data erased by the virus trap computer system includes one of, one computer software program within said second computer system(see col. 6, lines 8-22).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 5-7, 16-18, 23-24, 27, 29, 34-35, 40-41, 44-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schnurer et al in view of Templeton(6,401,210).

15. As per claims 5, 16, 34, 40 Schnurer et al. discloses wherein after said second computer system has deleted said intrusion by erasing data within said second computer system(see col. 8, lines 27-35). Schnurer et al. does not disclose said second computer system is capable of receiving a clean version of data that existed in said second computer system before said intrusion occurred. However, Templeton does disclose said second computer system(i.e. virus bin) is capable of receiving a clean version of data that existed in said second computer system(i.e. virus bin) before said intrusion occurred(see col. 3, lines 13-27, 50-56) . It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Schnurer et al. with Templeton to include receiving a clean version of data that existed in said second computer system before said intrusion occurred, the motivation is that an anti-virus program can clean the infected file, thereby restoring the file to its original functional state(see col. 1, lines 34-36 of Templeton), Templeton places infected files in a virus bin so that the virus cannot infect the computer system, thus, Templeton anti-virus techniques manage files containing computer viruses, by restoring the infected file(see col. 2, lines 38-44, col. 4, lines 41-55 of Templeton).

16. As per claims 6, 17, 27, 35 same motivation applies above(see claim 5). Schnurer et al. does not disclose wherein said second computer system comprises a restoration controller capable of supplying to said second computer system said clean version of said data after said second computer system has deleted said intrusion by erasing data within said second computer system. However, Templeton discloses said second computer system inherently includes a restoration controller capable of supplying to said second computer system said clean version of said data after said second computer system has deleted said intrusion by erasing data within said second computer system, because Templeton discloses that a virus bin is a repository of where infected files are placed(see col. 2, lines 45-48), and where the system is protected from spreading of the virus(see col. 3, lines 22-24). Templeton discloses that a infected file may be restored, thus Templeton inherently discloses a restoration controller, because Templeton discloses the clean option attempts to remove the virus from the file and then restore the file to its original location(see col. 4, lines 50-53) . As per claim 27, limitations have already been addressed (see claim 6, 23-24).

17. As per claims 7, 18, 41 Schnurer discloses wherein the second computer system(i.e. virus trap) is capable of receiving the clean version of the data from the first computer system(i.e. file server)(see col. 6, lines 41-45, col. 8, lines 26-35).

18. As per claims 23, 44, Schnurer discloses the virus trap computer system includes a mass storage device coupled to said embedded personal computer(see col. 6, lines 8-40). Schnurer does not disclose a restoration controller said restoration controller capable of (1) causing all data on said embedded personal computer and said mass storage device to be erased, and (2) after said data has been erased, supplying a clean version of said erased data to said embedded

personal computer and to said mass storage device. However, Templeton does discloses a restoration controller said restoration controller capable of (1) causing all data on said embedded personal computer and said mass storage device to be erased(see col. 2, lines 45-48), and (2) after said data has been erased, supplying a clean version of said erased data to said embedded personal computer and to said mass storage device(see col. 4, lines 50-53) . It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Schnurer et al. with Templeton to include receiving a clean version of data that existed in said second computer system before said intrusion occurred, the motivation is that an anti-virus program can clean the infected file, thereby restoring the file to its original functional state(see col. 1, lines 34-36 of Templeton), Templeton places infected files in a virus bin so that the virus cannot infect the computer system, thus, Templeton anti-virus techniques manage files containing computer viruses, by restoring the infected file(see col. 2, lines 38-44, col. 4, lines 41-55 of Templeton).

19. As per claims 24, 45, Schnurer discloses the virus trap computer system(see col. 6, lines 41-49). Schnurer inherently discloses a mass storage integrity controller, because Schnurer discloses that all files are executed inside the emulation box of the virus trap, where CRC is done(see col. 7, lines 39-47); capable of detecting an intrusion on said mass storage device(see col. 7, lines 39-67, col. 8, lines 27-35). Schnurer does not disclose requesting said embedded personal computer to cause said restoration controller to cause all data on said mass storage device to be erased. However, Templeton does disclose requesting said embedded personal computer to cause said restoration controller to cause all data on said mass storage device to be erased(see col. 2, lines 45-48, col. 4, lines 50-53). It would have been obvious to one of ordinary

skill in the art at the time of the invention was made to modify Schnurer et al. with Templeton to include receiving a clean version of data that existed in said second computer system before said intrusion occurred, the motivation is that an anti-virus program can clean the infected file, thereby restoring the file to its original functional state(see col. 1, lines 34-36 of Templeton), Templeton places infected files in a virus bin so that the virus cannot infect the computer system, thus, Templeton anti-virus techniques manage files containing computer viruses, by restoring the infected file(see col. 2, lines 38-44, col. 4, lines 41-55 of Templeton).

20. As per claim 29, Schnurer discloses wherein the embedded personal computer is the mass storage integrity controller(see col. 7, lines 39-47). Schnurer does not disclose a restoration controller. Templeton discloses a restoration controller, because Templeton discloses that a infected file may be restored, thus Templeton inherently discloses a restoration controller, because Templeton discloses the clean option attempts to remove the virus from the file and then restore the file to its original location(see col. 4, lines 50-53) . It would have been obvious for one of ordinary skill in the art at the time of the invention to include the restoration controller and mass storage integrity controller on one integrated chip, the motivation is that if both are integrated on the same chip, it is more of an efficient method.

21. Claims 8, 10-11, 19, 21-22, 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schnurer et al in view of Reardon(5,434,562).

22. As per claims 8, 19, Schnurer et al. does not disclose wherein the second computer system includes a peripheral switch that is capable of switching control of at least one computer peripheral from the second computer system to the first computer system and from the first

computer system to the second computer system. However, Reardon discloses wherein the second computer system includes a peripheral switch that is capable of switching control of at least one computer peripheral from the second computer system to the first computer system and from the first computer system to the second computer system(see col. 3, lines 37-48, col. 4, lines 31-47). It would have been obvious to one or ordinary skill in the art at the time of the invention to include the peripheral switch that is capable of switching control of at least one computer peripheral of Templeton with Schnurer et al., the motivation is that by providing complete control over a computer's access to its peripheral devices, allows the user to implement greater security precautions against unauthorized programs or users(see col. 1, lines 45-53 of Templeton, see col. 1, lines 9-44).

23. As per claims 10, 21, 43, Schnurer discloses the second computer system includes an embedded personal computer(i.e. virus trap)(see col. 6, lines 8-40). However, Schnurer et al. does not disclose a data transfer switch. Reardon discloses wherein the second computer system includes an embedded personal computer, a data transfer switch(see col. 2, lines 39-53, col. 3, lines 37-65), a data transfer switch coupled to the embedded personal computer and to the first computer system(see col. 4, lines 13-31), wherein the data transfer switch is capable of transferring data from the first computer system to the embedded personal computer when the data transfer switch is set in read only mode(see col. 6, lines 11-22); and wherein the data transfer switch is capable of transferring data from the embedded personal computer to the first computer system and from the first computer system to the embedded personal computer when the data transfer switch is set in read and write mode(see col. 3, lines 56-65, col. 5, lines 1-22, 32-65). It would have been obvious to one of ordinary skill in the art at the time of the invention

to include the data transfer switch of Reardon with Schnurer, the motivation is that a data transfer switch that can make certain portions of the computer to read-only, write-only, provide security precautions against unauthorized programs or users(see col. 1, lines 45-53 or Reardon).

24. As per claims 11, 22, same motivation applies above(see claim 10). Reardon discloses wherein the data transfer switch is exclusively controlled by the first computer system(see col. 4, lines 13-31).

25. As per claims 25-26, 28, 30, 46-47 are objected to as being rejected on base claims. The claims are objected to for the limitation of a password controller, and receiving a computer communication in the password controller and in response to receiving a valid password allowing computer communication to the embedded password. Prior art nor patent literature discloses or teaches the embedded computer allowing communication with a password. Schnurer discloses a virus trap computer, that executes files within the computer to prevent infection to the file server. Schnurer does not disclose allowing access to the virus trap computer with a password.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JJ
September 23, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100